REMARKS

Claims 8, 10-15, 17-18 and 21-22 are now pending in the application. As suggested by the Examiner, Claims 8 and 15 are amended to incorporate the limitations of claims 21 and 22, along with the formal definitions at page 8, lines 1-15, and to show how the inclusion thereof affects the utility of the invention. Applicant requests cancellation of claims 10-12, 17-18, and 21-22 without prejudice or disclaimer of the subject matter recited therein. Applicant requests addition of new claims 23 -26, which separately recite structural limitations to a content provider and player device. Support for the amendments and new claims may be found in the specification as originally filed at pages 8-10, and in the originally filed claims. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

REJECTION UNDER 35 U.S.C. § 103

Claims 8, 10-15, 17-18 and 21-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Moskowitz et al. (U.S. Pat. No. 5,745,569) in view of Leighton (U.S. Pat. No. 5,949,885), further in view of Rhoades (U.S. Pat. No. 5,745,569), and yet further in view of Barton (U.S. Pat. No. 6,047,374). This rejection is respectfully traversed.

As explained in detail below, none of the references cited by the Examiner teach active data and control data embedded in a host data signal. Art cited by the Examiner primarily relates to use of digital watermarks, which are defined in Applicant's specification as originally filed at page 1, lines 16-18 as passive data. In contrast,

Applicant's claimed invention relates to hiding active data defined in the specification and claims as executable machine instructions. Although Moskowitz et al. refers to its active data as a type of "digital watermark", this particular definition of Moskowitz et al. does not carry over to Applicant's claimed invention, nor to the other cited references, which clearly refer to passive data when using the word "digital watermark". The difference is significant because, unlike digital watermarks, executable machine instructions are highly sensitive to any errors, making errorless extraction of paramount importance. Accordingly, none of the cited references teach, suggest, or motivate that it is even possible to embed both active and error correction data in a host audio media stream, much less enable such embedding in a hidden manner that avoids perception to the human auditory system.

The Examiner relies on Moskowitz et al. to teach active hidden data and control data embedded in a host signal. The license key in Moskowitz et al. that the Examiner identifies as control data is used to determine different positions in the host data signal within which different sets of active data ("essential code resources") are hidden; the key is embodied in the selection of positions in the host signal in which the active data is hidden, but is not actually embedded in the host signal, at least not in a same portion of the host signal as the active data. In the case where the key is the license code, (Column 6, lines 1-3) then if the key were embedded in the host signal, the purpose of the teachings of Moskowitz et al. would be thwarted, since the user would not have to type in the license code distributed with the hardcopy of the software to derive the key, but could extract it from the softcopy. In the case where the key is stored as a code resource, but encrypted with a derivative of the license code (Column 6, lines 9-22),

then the key is still not embedded in a same portion of the host data signal as the active data, but as its own "data resource". Even if one were to embed the encrypted key in the host data signal, which Moskowitz et al. does not suggest, then Moskowitz still only teaches embedding different "resources" in different portions of the host data signal, and does not suggest that it is possible, nor enable how, to hide control data in a portion of the host data signal that is embedded with the active data, without interfering with bits of the extremely error-sensitive active data. Thus, Moskowitz et al. does not hide two different sets of active data and control data in a same portion of the host signal; rather, the need to avoid interference between bits is avoided by only embedding different portions of one set of data in discrete locations that vary according to the license key. This technique is not suitable for embedding error correction data, especially while avoiding interference between bits of different sets of active data and error correction data embedded in same portions of the host signal.

The Examiner relies on Rhoades to provide an example of orthogonal embedding of control data (a "copy never" bit contained in a second watermark) respective of active data, which is actually passive data (a first watermark of which the second watermark is a copy). The "copy never" bit is just binary license information, and not an executable instruction; rather, the executable instructions must be on the compliant machine that references the variable data stored in the "copy never" bit. If one were to modify Rhoades by replacing one of the digital watermarks with active hidden data, then the functionality of Rhoades (orthogonally embedding an extracted copy) would be destroyed; Rhoades extracts the first embedded watermark from the received signal, copies the first watermark as a second watermark having a "copy

never" bit asserted, and embeds the second watermark orthogonally to the first watermark to increase the likelihood that the second water mark will be detected. Thus, Rhoades cannot be permissibly combined with Moskowitz et al. to arrive at Applicant's claimed invention, because there can be no suggestion or motivation to modify Rhoades, nor to modify Moskowitz et al. based on the teachings of Rhoades (*see* MPEP 2143.01 "The Proposed Modification Cannot Render the Prior Art Unsatisfactory for Its Intended Purpose"). Moreover, Moskowitz et al. cannot be modified based on the teachings of Rhoades to embed the license key orthogonally to the active data, because it would defeat the security measure of forcing the user to type in the written license code distributed with the hardcopy of the software as explained above.

Also, Rhoades copies the first watermark and embeds it as a second watermark containing the control data orthogonal to the first watermark, which makes the first watermark expendable. For example, Rhoades teaches that it is advantageous if the first watermark is weakened by corruption of the pre-transmitted host signal, because the second watermark is more easily detected since it is native to the corrupted signal (column 22, lines 52-30). Rhoades even goes so far as to say that the corruption of the first watermarked signal contributes to the orthogonality of the two watermarks, so that the two watermarks will not have the same time base or other foundation. Thus, Rhoades teaches that the first watermark is no longer important once the second watermark is embedded, and inherently teaches away from ensuring errorless extraction of the first watermark by orthogonal embedding of its copy containing the control data (i.e., the copy never bit equating to binary licensing information). Accordingly, it is not obvious to replace the passive data of the first watermark in

Rhoades with active data according to Moskowitz et al., because Rhoades teaches that the first watermark is no longer of interest, and should be ignored ("Compliant equipment must ... refuse to copy if ***either*** is found to have the 'copy never' bit asserted." Emphasis added. Column 52, lines 19-21). It follows that there can be no teaching, motivation, or suggestion to add orthogonal embedding of control data to Moskowitz et al. based on Rhoades, because Rhoades teaches orthogonal embedding in a way (after receipt of the transmitted and hopefully corrupted signal) that is not consistent with an attempt to ensure errorless extraction of any hidden data (active or passive) embedded in the original and hopefully corrupted signal (unless the orthogonally embedded data is a copy). As a result, neither Moskowitz et al. nor Rhoades teach, suggest, or motivate that active data and its error extraction data can be successfully hidden in a host data signal in an extractable fashion by orthogonal embedding of one with respect to the other, especially because Rhoades teaches making a copy of the first data and embedding it again in the signal as second data orthogonal to the first data, and its control data contained in the second data governs control of active data that is not even embedded in the signal.

Further, Rhoades only discloses orthogonal embedding in transform coefficients and in samples in the temporal or spatial domains (column 52, lines 31-42). In contrast, Applicant's claimed invention embeds the error sensitive active data and its error correction data in singular points and maskee points of same portions of the host data. As a result, the perceptibility of the embedded data to the human ear is minimized, while the detectability of both sets of the embedded data by a machine is maximized by avoiding interference between embedded bits; as a result, extractability of each layer of

active hidden data and error correction data is ensured, so that the errorless extraction of the active data can be achieved.

The Examiner only relies on Leighton and Barton to teach error correction coding and embedding of authentication data. At one point (Column 5, lines 52-55), Leighton discusses orthogonal embedding of a base watermark respective to an offset copy of itself. Still, only passive data is embedded, and Leighton goes on to suggest an ***improvement*** whereby the base watermark can be discarded (Column 5, line 57 – column 6, line 34). Thus, Leighton implicitly teaches away from this technique, even in the case where only passive data (which is more resilient to error than active data) is embedded. Nor does Leighton disclose how orthogonal embedding takes place, or even suggest that it is possible to ensure errorless extraction of one set of data by using the other set of data, while effectively hiding both sets of data from human auditory perception. Accordingly, neither Leighton nor Barton, either alone or combined with one another or the other references, teach suggest, or motivate embedding active data and error correction data in same, embedded portions of a host audio media signal to ensure imperceptibility to human hearing and errorless extraction of the active hidden data.

Accordingly, the differences between the teachings of Rhoades and Applicant's claimed invention are significant, and none of the other cited references provide the recited subject matter in claims 1 and 15, especially as amended.

Applicant requests the Examiner withdraw the rejection of claims 1 and 15 under 35 U.S.C. § 103(a), along with rejection on these grounds of all claims dependent therefrom.

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: July 2, 2004

By: _____
Gregory A. Stobbs, Reg. #28,764
Jennifer S. Brooks, Reg. #51,501

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600